WHAT IS CLAIMED

1. A method for authenticating a first party at a second party, comprising:

(a) receiving a random number from said first party as a first challenge;

(b) incrementing a count value in response to receiving said first challenge;

(c) generating a first challenge response by performing a keyed cryptographic function (KCF) on said first challenge and said count value using a first key;

(d) transferring said count value, as a second challenge, and said first challenge response to said first party;

(e) receiving a second challenge response from said first party, said second challenge response being a result of performing said KCF on said second challenge using said first key; and

(f) verifying said first party based on said second challenge and said second challenge response.

2. The method of claim 1, prior to said step (c), further comprising:

(g) generating said first key using a root key.

3. The method of claim 1, wherein said step (c) generates said first challenge response by performing said KCF on said first challenge, said count value, and an identifier for said second party using said first key.

4. The method of claim 1, further comprising:

(g) establishing a second key based on said first and second challenges.

Sub A1

5. The method of claim 1, wherein said step (a) eceives a global challenge as said first challenge from said first party.

6. The method of claim 1, wherein said first party is a network of a wireless system and said second party is a mobile.

7. The method of claim 6, wherein said step (c) generates said first challenge response by performing said KCF on said first challenge, said count value and type data using said first key, said type data indicating a type of protocol being performed by said network and said mobile.

8. The method of claim 6, wherein said step (c) generates said first challenge response by performing said KCF on said first challenge, said count value, an identifier for said mobile, and type data using said first key, said type data indicating a type of protocol being performed by said network and said mobile.

9. The method of claim 6, further comprising:

(g) establishing a second key based on said first and second challenges.

10. The method of claim 9, wherein said second key is one of secret shared data and a session key.

11. The method of claim 6, wherein said step (b) increments said count value using a bit counter of greater than 64 bits and which was initialized using a random number.

12. A method for authenticating a first party at a second party, comprising:

(a) outputting a random number as a first challenge;

(b) receiving a second challenge and a first challenge response from said first party, said second challenge being a count value, and said first challenge response being a result of performing a keyed cryptographic function (KCF) on said first challenge and said count value using a first key; and

(e) verifying said first party based on said first challenge, said second challenge, and said first challenge response.

13. The method of claim 12, further comprising:

(f) establishing a second key based on said first and second challenges.

14. The method of claim 12, wherein said step (a) outputs said first challenge as a global challenge.

15. The method of claim 12, wherein said first party is a mobile of a wireless system and said second party is a network.

16. The method of claim 15, further comprising:

(f) establishing a second key based on said first and second challenges.

17. The method of claim 16, wherein said second key is one of secret shared data and a session key.

18. The method of claim 12, further comprising:

(f) generating a second challenge response by performing said KCF on said second challenge using said first key; and

(g) transferring said second challenge response to said second party.

19. The method of claim 18, wherein said step (f) generates said second challenge response by performing said KCF on said second challenge and an identifier for said second party using said first key.

20. The method of claim 18, wherein said first party is a mobile of a wireless system and said second party is a network.

21. The method of claim 20, wherein said step (f) generates said second challenge response by performing said KCF on said second challenge and type data using said first key, said type data indicating a type of protocol being performed by said network and said mobile.

22. The method of claim 20, wherein said step (f) generates said second challenge response by performing said KCF on said second challenge, an identifier for said network, and type data using said first key, said type data indicating a type of protocol being performed by said network and said mobile.